



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,850	09/23/2005	Arnaud Dahamel	034512-001	7093
21839 7590 08/28/2008 BUCHANAN, INGERSOLL & ROONEY PC POST OFFICE BOX 1404 ALEXANDRIA, VA 22313-1404				
EXAMINER				
SQUIRES, BRETT S				
ART UNIT		PAPER NUMBER		
2131				
NOTIFICATION DATE		DELIVERY MODE		
08/28/2008		ELECTRONIC		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

# Office Action Summary

**Application No.**

10/549,850

**Applicant(s)**

DAHAMEL ET AL.

**Examiner**

BRETT SQUIRES

**Art Unit**

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 23 September 2005.  
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 9-14 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 9-14 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☒ The specification is objected to by the Examiner.  
10) ☒ The drawing(s) filed on 26 September 2005 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☒ None of:  
1. ☒ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☒ Information Disclosure Statement(s) (PTO-8508)  
Paper No(s)/Mail Date 09/23/05  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_  
5) ☐ Notice of Informal Patent Application  
6) ☐ Other: \_\_\_\_\_

***Priority***

1. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in France on March 24, 2003. It is noted, however, that applicant has not filed a certified copy of the FR 03/03522 application as required by 35 U.S.C. 119(b). The applicant has instead submitted a certified copy of foreign application FR 02/02848 filed in France on March 6, 2002 and titled "Shelter for Fruit Trees Comprising Abutted Greenhouse Units Rigidified with Riggging and Equipped with Means for Tensioned Unfolding or Foldable Roofs." The foreign application FR 02/02848 filed March 6, 2002 does not support the applicant's claim for foreign priority.

***Drawings***

2. The drawing is objected to under 37 CFR 1.83(a). The drawing must show every feature of the invention specified in the claims. Therefore, the cache memory and the cache memory controller must be shown or the feature(s) canceled from the claim(s). No new matter should be entered. The examiner respectfully points out that the cache memory and the cache memory controller are essential for understanding the invention because they adapt the length of data processed by the security module to the standard data length.

The drawing is objected to because text labels are necessary for the applicant's drawings to be understood. The applicant's drawing contains rectangular boxes and an oval whose meanings are unclear instead of conventional drawing symbols whose meanings are readily apparent, such as the circuit elements that represent resistors,

capacitors, or inductors. Accordingly, the rectangular boxes should have text labels for clarification purposes.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### ***Specification***

3. The disclosure is objected to because of the following informalities: multiple are designations are given to the same element in figure 1 ref. no. CR. This element referred to as the encryption means CR on page 3 line 19 and a security module CR on page 4 line 20. Appropriate correction is required.

***Claim Objections***

4. Claim 1 is objected to because of the following informalities: claim 1 recites "a set of peripheral devices including at least one communication interface for external access, wherein said peripherals, unlike said communication interface," this contradictory language makes it unclear whether or not the communication interface is included in the set of peripherals. Appropriate correction is required.

***35 USC § 112, sixth paragraph***

5. Claim 1 satisfies the three-pronged analysis necessary to invoke 35 U.S.C. § 112, sixth paragraph and accordingly this claims are interpreted as means-plus-function claims. The three-pronged analysis necessary to invoke 35 U.S.C. § 112, sixth paragraph is recited below:

A claim limitation will be presumed to invoke 35 U.S.C. 112, sixth paragraph, if it meets the following 3-prong analysis:

- (A)the claim limitations must use the phrase "means for" or "step for;"
- (B)the "means for" or "step for" must be modified by functional language; and
- (C)the phrase "means for" or "step for" must not be modified by sufficient structure, material, or acts for achieving the specified function.

***Claim Rejections - 35 USC § 102***

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 9-14 are rejected under 35 U.S.C. 102(b) as being anticipated by Ma et al. (US 6,996,725).

Regarding Claim 9:

Ma discloses an integrated circuit ("Microcontroller" See fig. 2A ref. no. 100) having a microprocessor ("CPU" See fig. 2A ref. no. 235) and a set of peripheral devices ("Decryptor," "Decrypted Buffer," and "Cache" See fig. 2A ref. nos. 220, 225, and 230) including at least one communication interface for external access ("I/O Buffer" See fig. 2A ref. no. 215), wherein said peripherals unlike the communication interface, are connected to the microprocessor by an interconnection bus ("Internal Bus" See fig. 2A ref. no. 240) on which the data length is equal to the standard data length of the data processed by the microprocessor ("The CPU processes one byte instructions." See col. 2 lines 6-34 and "The internal bus is 8-bits wide." See col. 6 lines 47-48), the integrated circuit also has a security module ("Decryptor" See fig. 2A ref. no. 220) connected to the interconnection bus and the communication interface by a dedicated link ("The connection between the Decryptor and the Decrypted Buffer and the connection between the Decryptor and the I/O Buffer." See figure 2A), wherein the length of the data processed by the security module is greater than the standard data length of the data processed by the microprocessor ("Program decryption may be effectuated on block of 64-bits" See fig. 2B ref. no. 220, col. 4 lines 58-67, col. 5 lines 1-23, and col. 6 lines 25-34), and the integrated circuit has means for adapting the length of the data

process by the security module to the standard length ("Decrypted Buffer," "Cache," and "Memory Controller" See fig. 2A ref. nos. 225, 230, fig. 4 ref. no. 405, col. 4 lines 30-36 and 53-57, col. 5 lines 20-23).

Regarding Claim 10:

Ma discloses the means for adapting the length of data processed by the security module to the standard data length includes a cache memory ("Cache" See fig. 2A ref. no. 230) associated with the microprocessor and provided with a cache memory controller ("Memory Controller" See fig. 4 ref. no. 405) which upon accessing the cache memory causes it to transmit to the security module data having a length equal to the standard data length whereby the processing of the data by the security module is performed on the fly ("The memory controller may be responsible for coordinating the internal address bus and the internal data bus activities, the cache/tag access and update, program block decryption, and external data/program memory accesses (See col. 6 lines 20-24).

Regarding Claim 11:

Ma discloses block encryption scheme that relies on caching blocks of instructions so the when encryption is performed on multiple instructions/bytes simultaneously the occurrence of stalls of the microcontroller is minimized (See col. 3 lines 32-46).

Regarding Claim 12:

Ma discloses during the deciphering of the data by the security module, the cache memory breaks the deciphered data available at the output of the security

module which has a length greater than the standard data length into standard-length data ("The CPU may wait until the decrypted instructions are stored in the cache and then the cache transmits a one byte instruction to the CPU upon request by the CPU." See col. 2 lines 6-34 and col. 5 lines 20-23).

Regarding Claim 13:

Ma discloses decryptor uses a secret key algorithm which processes data having a length of at least 64-bits and wherein the standard length of the data processed by the microprocessor is less than 64-bits ("The CPU processes one byte instructions." See col. 2 lines 6-34 and "The microcontroller may be designed to decrypt a 64-bit block in five machine cycles for single DES operations." See col. 6 lines 25-34).

Regarding Claim 14:

Ma discloses a block encryption scheme using the AES algorithm (See col. 3 lines 20-25).

### ***Conclusion***

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRETT SQUIRES whose telephone number is (571) 272-8021. The examiner can normally be reached on 9:00am - 5:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BS/  
/Ayaz R. Sheikh/  
Supervisory Patent Examiner, Art Unit 2131